REMARKS

The Office Action mailed April 23, 2003, has been carefully reviewed, and the foregoing amendments and following remarks are made in consequence thereof.

Claims 1-22 are now pending in this application. Claims 1-22 stand rejected.

The rejection of Claims 1-4, 6, 7, and 9-22 under 35 U.S.C. § 102(e) as being anticipated by Lightbody et al. (U.S. Patent No. 6,000,034) is respectfully traversed.

Lightbody et al. describe a security system for a programmable revenue class electricity meter. The programming can be changed by authorized persons to modify meter values or parameters. The security system checks for a code word that is required to be input by authorized persons prior to any changes in the revenue-related programming. The security system compares the input code to a code word stored in the meter and unlocks restrictions on modification of the revenue-related programming if the input code word matches the stored code word. After the parameters and values in the meter have been modified, the modification is stored as a transaction in an event log. The event log records all transactions wherein modification of the parameters or values in the meter has been made and whether security has been enabled/disabled. The event log also records the date and time of the access. The event log can also record the key used to enable or disable the security thereby enabling identification of the user who has gained access or altered the configuration of the meter. Accordingly, the event log can be used as a security backup to detect any unauthorized accesses to the meter.

Claim 1 recites a method for creating a secure program history log for a programmable device including a microprocessor, at least one communications port for communicating with the microprocessor and at least one memory device electrically connected to the microprocessor, the memory device including a program history log to monitor an accuracy of input program parameters wherein the method includes "communicating input program parameters to the microprocessor in a programming event...creating a log entry utilizing the microprocessor and the program parameters as the

input program parameters are communicated...writing the log entry into the program history log utilizing the microprocessor such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable."

Lightbody et al. do not describe nor suggest a method that includes communicating input program parameters to the microprocessor in a programming event, creating a log entry utilizing the microprocessor and the program parameters as the input program parameters are communicated, and writing the log entry into the program history log utilizing the microprocessor such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable. Specifically, Lightbody et al. do not describe nor suggest creating a log entry utilizing the microprocessor and the program parameters as the input program parameters are communicated. Rather, in contrast to the present invention, Lightbody et al. explain at Column 14, lines 50-52, "[a]fter the parameters and values in the meter have been modified, the modification is stored as a transaction in an event log." Moreover, Lightbody et al. do not describe nor suggest writing the log entry into the program history log utilizing the microprocessor such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable. Rather, in contrast to the present invention, Lightbody et al. explain at Column 14, lines 53-61:

> [t]his event log 489 records all transactions wherein modification of the parameters or values in the meter has been made and whether security has been enabled/disabled. The event log also records the date and time of the access. The event log can also record the key used to enable or disable the security thereby enabling identification of the user who has gained access or altered the configuration of the meter. Accordingly, the event log can be used as a security backup to detect any unauthorized accesses to the meter.

Lightbody et al. do not describe nor suggest a meter that saves enough information to identify changes to the meter parameters and to restore the changes if the changes were unauthorized. Accordingly, for at least the reasons set forth above, Claim 1 is submitted to be patentable over Lightbody et al.

For the reasons set forth above, Applicants respectfully requests that the Section 102 rejection of Claim 1 be withdrawn.

Claims 2-4, 6, 7, and 9-11 depend, directly or indirectly, from independent Claim 1. When the recitations of 2-4, 6, 7, and 9-11 are considered in combination with the recitations of Claim 1, Applicants submit that dependent Claims 2-4, 6, 7, and 9-11 likewise are patentable over Lightbody et al.

Claim 12 recites a system for creating a secure program history log for a programmable device including "at least one communications port, said communications port configured to receive inputs comprising program input parameters in a programming event, said program input parameters employed to generate data outputs from the programmable device...a microprocessor configured to receive said program input parameters from said communications port and create a log entry based on said program input parameters to monitor changed program input parameters_such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable...at least one memory device electrically connected to said microprocessor and comprising said program history log, said microprocessor further configured to write said log entry into said program history log, thereby protecting said program history log from manipulation via direct communication from said communications port."

Lightbody et al. do not describe nor suggest a system for creating a secure program history log for a programmable device including a microprocessor configured to receive program input parameters from the communications port and create a log entry based on the program input parameters to monitor changed program input parameters such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable. Specifically, Lightbody et al. do not describe nor suggest a microprocessor configured to receive program input parameters from the communications port and create a log entry based on the program input parameters to monitor changed program input parameters such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable. Rather, in contrast to the present invention, Lightbody et al. explain at Column 14, lines 53-61:

> [t]his event log 489 records all transactions wherein modification of the parameters or values in the meter has been made and whether security has been enabled/disabled. The event log also records the date and time of the access. The event log can also record the key used to enable or disable the security thereby enabling identification of the user who has gained access or altered the configuration of the meter. Accordingly, the event log can be used as a security backup to detect any unauthorized accesses to the meter.

Lightbody et al. do not describe nor suggest a meter that saves enough information to identify changes to the meter parameters and to restore the changes if the changes were unauthorized. Accordingly, for at least the reasons set forth above, Claim 12 is submitted to be patentable over Lightbody et al.

For the reasons set forth above, Applicants respectfully requests that the Section 102 rejection of Claim 12 be withdrawn.

Claims 13-15, depend, directly or indirectly, from independent Claim 12. When the recitations of Claims 13-15 are considered in combination with the recitations of Claim 12, Applicants submit that dependent Claims 13-15 likewise are patentable over Lightbody et al.

Claim 16 recites an electronic electricity meter including "a communications port, said communications port configured to receive meter input parameters in a programming event...a microprocessor configured to receive said meter input parameters from said communications port and determine energy consumption data outputs based upon said meter input parameters, said microprocessor further configured to create a program history log entry when meter input parameters are received in the programming event...at least one memory device electrically connected to said microprocessor and comprising a program history log to record changes to meter input parameters, said microprocessor further configured to write said log entry into said program history log such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable."

Lightbody et al. do not describe nor suggest a meter including a microprocessor configured to write said log entry into said program history log such that changes to meter

parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable. Rather, in contrast to the present invention, Lightbody et al. explain at Column 14, lines 53-61:

> [t]his event log 489 records all transactions wherein modification of the parameters or values in the meter has been made and whether security has been enabled/disabled. The event log also records the date and time of the access. The event log can also record the key used to enable or disable the security thereby enabling identification of the user who has gained access or altered the configuration of the meter. Accordingly, the event log can be used as a security backup to detect any unauthorized accesses to the meter.

Lightbody et al. do not describe nor suggest a meter that saves enough information to identify changes to the meter parameters and to restore the changes if the changes were unauthorized. Accordingly, for at least the reasons set forth above, Claim 16 is submitted to be patentable over Lightbody et al.

For the reasons set forth above, Applicants respectfully requests that the Section 102 rejection of Claim 16 be withdrawn.

Claims 17-19 depend from independent Claim 16. When the recitations of Claims 17-19 are considered in combination with the recitations of Claim 16, Applicants submit that dependent Claims 17-19 likewise are patentable over Lightbody et al.

Claim 20 recites an electronic electricity meter including "a microprocessor configured to determine energy consumption output data based upon at least one meter input parameter received in a programming event...at least one memory device electrically connected to said microprocessor and comprising a program history log for recording an occurrence of said programming event...a communications port, said communications port configured to receive said at least one meter input parameter for use by said microprocessor to generate output data; said microprocessor configured to create a program history log entry and configured to write said log entry into said program history log when said at least one meter parameter is received in said programming event, said program history log comprising at least one of an entry sequence number, a transaction number, a date and time stamp, and a

table identifier such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable."

Lightbody et al, do not describe nor suggest an electronic electricity meter configured to determine energy consumption output data based upon at least one meter input parameter received in a programming event, and a communications port wherein the communications port is configured to receive at least one meter input parameter for use by the microprocessor to generate output data wherein the microprocessor is configured to create a program history log entry and configured to write the log entry into the program history log when at least one meter parameter is received in the programming event, the program history log including at least one of an entry sequence number, a transaction number, a date and time stamp, and a table identifier, such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable. Rather, in contrast to the present invention, Lightbody et al. explain at Column 14, lines 53-61:

> [t]his event log 489 records all transactions wherein modification of the parameters or values in the meter has been made and whether security has been enabled/disabled. The event log also records the date and time of the access. The event log can also record the key used to enable or disable the security thereby enabling identification of the user who has gained access or altered the configuration of the meter. Accordingly, the event log can be used as a security backup to detect any unauthorized accesses to the meter.

Lightbody et al. do not describe nor suggest a meter that saves enough information to identify changes to the meter parameters and to restore the changes if the changes were unauthorized. Accordingly, for at least the reasons set forth above, Claim 20 is submitted to be patentable over Lightbody et al.

For the reasons set forth above, Applicants respectfully requests that the Section 102 rejection of Claim 20 be withdrawn.

Claims 21-22 depend from independent Claim 20. When the recitations of Claims 21-22 are considered in combination with the recitations of Claim 20, Applicants submit that dependent Claims 21-22 likewise are patentable over Lightbody et al.

For the reasons set forth above, Applicants respectfully request that the Section 102 rejection of Claims 1-4, 6, 7, and 9-22 be withdrawn.

The rejection of Claims 5 and 8 under 35 U.S.C. § 103 as being unpatentable over Lightbody et al. in view of Bui et al. (U.S. Patent No. 6,532,128) is respectfully traversed.

Lightbody et al. is described above. Bui et al. describe a longitudinal media drive 12 employed in data processing systems as a secondary storage media for storing large amounts of data for low cost, infrequently used data or for archival purposes wherein the drive records data on a high speed moving recording media which is subject to stoppage, such as a tape. The drive system further correlates data processing data sets to the media position and resynchronizes the media position to the data set sequence upon restart of the media movement. Specifically, the data (in the form of a series of data sets) is transferred to the longitudinal media for writing on the media by streaming. Similarly, the data is often read on a continuous basis. The data transfer is, however, subject to interruption or to a temporary fault condition while the media continues to move at its continuous nominal velocity. Thus, the media must be stopped, and later restarted. On restart, the media position must be correlated and resynchronized with respect to the data set sequence. A linear position generation logic 50 continuously reads and interpolates linear position registration data modulated into a prerecorded servo pattern on the recording media, and supplies read and interpolated position information (LPOS) to a data formatter 54. In data formatter 54, the read data flow of the read/write channel of drive 12 decodes a set of unique characters recorded with each data set called the "Code Word Pair Header ID". The data formatter provides a hardware memory buffer and builds a table 57 of the relevant part of the most recent Code Word Pair Header ID's vs. LPOS. When a data set separator is detected, a new entry is made in the table 57, which, if the table is full, overwrites the oldest entry in the table.

Applicants respectfully submit that the Section 103 rejection of the presently pending claims is not a proper rejection. As is well established, obviousness cannot be established by combining the teachings of the cited art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. Neither Lightbody et al. nor

Bui et al., considered alone or in combination, describe or suggest the claimed combination. Furthermore, in contrast to the assertion within the Office Action, Applicants respectfully submit that it would not be obvious to one skilled in the art to combine Lightbody et al. with Bui et al., because there is no motivation to combine the references suggested in the art. Additionally, the Examiner has not pointed to any prior art that teaches or suggests to combine the disclosures, other than Applicants' own teaching. Rather, only the conclusory statement that "it would have been obvious to one of ordinary skill in the art, at the time of the invention, to modify Lightbody et al., so that data entries are overwritten, as taught by Bui et al., in order to be able to continue recording entries when the memory runs out of space" suggests combining the disclosures.

As the Federal Circuit has recognized, obviousness is not established merely by combining references having different individual elements of pending claims. Ex parte Levengood, 28 U.S.P.Q.2d 1300 (Bd. Pat. App. & Inter. 1993). MPEP 2143.01. Rather, there must be some suggestion, outside of Applicants' disclosure, in the prior art to combine such references, and a reasonable expectation of success must be both found in the prior art, and not based on Applicant's disclosure. In re Vaeck , 20 U.S.P.Q.2d 1436 (Fed. Cir. 1991). In the present case, neither a suggestion or motivation to combine the prior art disclosures, nor any reasonable expectation of success has been shown.

Furthermore, it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the cited art so that the claimed invention is rendered obvious. Specifically, one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the art to deprecate the claimed invention. Further, it is impermissible to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. The present Section 103 rejection is based on a combination of teachings selected from multiple patents in an attempt to arrive at the claimed invention. Specifically, Lightbody et al. is cited for its teaching of a memory log for recording data histories, and Bui et al. is merely cited for its teaching of a method of synchronizing data sets on a recording media that overwrites the oldest data entry with a new

entry when the cache or memory is full. Since there is no teaching nor suggestion in the cited art for the combination, the Section 103 rejection appears to be based on a hindsight reconstruction in which isolated disclosures have been picked and chosen in an attempt to deprecate the present invention. Of course, such a combination is impermissible, and for this reason alone, Applicants request that the Section 103 rejection be withdrawn.

In addition, as is well established, obviousness cannot be established by combining the teachings of the cited art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. Neither Lightbody et al. nor Bui et al., considered alone or in combination, describe or suggest writing a log entry into a program history log utilizing a microprocessor such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable.

If art "teaches away" from a claimed invention, such a teaching supports the nonobviousness of the invention. U.S. v. Adams, 148 USPQ 479 (1966); Gillette Co. v. S.C. Johnson & Son, Inc., 16 USPQ2d 1923, 1927 (Fed. Cir. 1990). In light of this standard, it is respectfully submitted that the cited are, as a whole, is not suggestive of the presently claimed invention. Moreover, Applicants respectfully submit that Bui et al. teach away from Lightbody et al. and the present invention, and as such, there is no suggestion or motivation to combine Bui et al. with Lightbody et al. Specifically, Bui et al. describe a method of registering data being recorded on a tape drive in a data processing system wherein a table in memory is populated with a set of unique characters recorded with each data set and respective interpolated linear position information such that when a data set separator is detected, a new entry is made in the table, which, if the table is full, overwrites the oldest entry in the table, and Lightbody et al. describe an event log that records all transactions wherein modification of the parameters or values in the meter has been made and whether security has been enabled/disabled.. In addition, neither Bui et al. nor Lightbody et al. describe nor suggest a program history log comprising at least one of an entry sequence number, a transaction number, a date and time stamp, and a table identifier such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable. Rather in contrast to the present invention, Lightbody et al.

describe a meter that does not enough information to identify changes to the meter parameters and to restore the changes if the changes were unauthorized, and Bui et al. describe a data processing tape drive system that only records a data set header and linear position data.

Moreover, and to the extent understood, no combination of Lightbody et al. and Bui et al., describe nor suggest the claimed invention. Specifically, Claim 1 recites a method for creating a secure program history log for a programmable device including a microprocessor, at least one communications port for communicating with the microprocessor and at least one memory device electrically connected to the microprocessor, the memory device including a program history log to monitor an accuracy of input program parameters wherein the method includes "communicating input program parameters to the microprocessor in a programming event...creating a log entry utilizing the microprocessor and the program parameters as the input program parameters are communicated...writing the log entry into the program history log utilizing the microprocessor such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable."

Neither Lightbody et al. nor Bui et al., considered alone or in combination, describe or suggest a method for creating a secure program history log for a programmable device including a microprocessor, at least one communications port for communicating with the microprocessor and at least one memory device electrically connected to the microprocessor, the memory device including a program history log to monitor an accuracy of input program parameters wherein the method includes "communicating input program parameters to the microprocessor in a programming event...creating a log entry utilizing the microprocessor and the program parameters as the input program parameters are communicated...writing the log entry into the program history log utilizing the microprocessor such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable." Specifically, neither Lightbody et al. nor Bui et al., considered alone or in combination, describe nor suggest creating a log entry utilizing the microprocessor and the program parameters as the input program parameters are communicated. Rather, in contrast to the present invention, Lightbody et al. explain at Column 14, lines 50-52, "[a]fter the parameters and values in the meter have been modified, the modification is stored as a

transaction in an event log" and Bui et al. describe that when a data set separator is detected, a new entry is made in a table. Moreover, neither Lightbody et al. nor Bui et al., considered alone or in combination, describe nor suggest writing the log entry into the program history log utilizing the microprocessor such that changes to meter parameters are identifiable, and if the changes are unauthorized, the meter parameters are restorable. Rather, in contrast to the present invention, Lightbody et al. explain at Column 14, lines 53-61:

> [t]his event log 489 records all transactions wherein modification of the parameters or values in the meter has been made and whether security has been enabled/disabled. The event log also records the date and time of the access. The event log can also record the key used to enable or disable the security thereby enabling identification of the user who has gained access or altered the configuration of the meter. Accordingly, the event log can be used as a security backup to detect any unauthorized accesses to the meter.

Lightbody et al. do not describe nor suggest a meter that saves enough information to identify changes to the meter parameters and to restore the changes if the changes were unauthorized, and Bui et al. describe a data processing tape drive system that only records a data set header and linear position data. For at least the reasons set forth above, Claim 1 is submitted to be patentable over Lightbody et al. in view of Bui et al.

Claims 5 and 8 depend from independent Claim 1. When the recitations of Claims 5 and 8 are considered in combination with the recitations of Claim 1, Claims 5 and 8 are likewise submitted to be patentable over Lightbody et al. in view of Bui et al.

For the reasons set forth above, Applicants respectfully requests that the Section 103 rejection of Claims 5 and 8 be withdrawn.

In view of the foregoing amendments and remarks, all the claims now active in this application are believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully Submitted,

William J. Zychlewicz
Registration No. 51,366
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070